UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/823,673 | 03/30/2001 | Taras Malivanchuk | 655/63957 | 6128 |

7590 03/07/2005

RICHARD F. JAWORSKI
Cooper & Dunham LLP
1185 Avenue of the Americas
New York, NY 10036

| EXAMINER | |
|---|---|
| ARANI, TAGHI T | |
| **ART UNIT** | **PAPER NUMBER** |
| 2131 | |

DATE MAILED: 03/07/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/823,673 | MALIVANCHUK ET AL. | |
| | Examiner | Art Unit | |
| | Taghi T. Arani | 2131 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *10 September 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

## DETAILED ACTION

1. Claims 1-24 were pending for examination.

### Response to Amendment

Applicant's arguments filed 9/10/2004 regarding the rejection of the claims 1-20 under 35 U.S.C. 102 and 103 have been fully considered but they are not persuasive.

As per Applicant's argument relating to Nachenberg reference with respect to the rejections of claims 1, 6, 11 and 16, Applicant states that Nachenberg reference relates to an emulation repair system that restores virus-infected computer files to their uninfected states and that Nachenberg's virus definition file including "RepairFile" data field used to specify a binary filename of an associated overlay program do not corresponds to the " recited art of retrieving from a data file, information relating to the malicious code including at least one command used for restoring the computer system to a state that existed prior to modification by the malicious code, as recited in amended independent claim 1".

The Examiner responds that Nachenberg's virus definition file (i.e. a data file) includes an index to an associated overlay file appropriate for the virus (col. 7, lines 61-65) which is used for decrypting the virus and for identifying an appropriate overlay module which includes code (i.e. command) for locating and co-opting virus repair code to restore host file [col. 9, lines 1-16, col. 8, lines 20-31). That is, the overlay module including code (indexed by the virus definition file) to restore the computer file corresponds to the broadest reasonable interpretation ((MPEP 904.01, See also In re Morris, 127 F.3d 1048, 44 USPQ2nd 1023 (Fed. Cir. 1997) of the recited "retrieving from a data file, information relating to the malicious code including at least one command used for restoring the computer system".

*Claim Rejections - 35 USC § 102*

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

2. **Claims 1-2, 5-7, 10-12 and 15-17 and 20** are rejected under 35 U.S.C. 102(e) as being anticipated by Nachenberg (IDS #5), US Pat. No. 6, 067, 410, files Feb. 1996.

**As per claims 1, 6, 11 and 16, 21-24,** Nachenberg is directed to an emulation repair system (ERS) which restores virus-infected computer files to their uninfected states [see abstract] comprising:

scanning the computer system for the malicious code [Nachenberg teaches scanning the computer system for the malicious (or virus) code and identifying the type of virus, see col. 6, lines 37-40, see also, col. 10, lines 33-54];

identifying the malicious code;

retrieving from a data file, information relating to the malicious code including at least

one command used for restoring the computer system to a state that exists prior to modification by the malicious code [Nachenberg teaches a virus definition file (i.e. a data file) comprising an entry or virus definition for each known virus. Each virus definition contains information specific to a virus or a family of such viruses, see col. 7, lines 54-57. That is, the ERS uses the virus type at input as an index to an appropriate virus definition in virus definition file, see col. 7, lines 58-60]; and

executing the at least one command to restore the computer system to the state as it existed prior to modification by the malicious code [Nachenberg further teaches that the virus definition of the virus definition file includes an index to an associated overlay file appropriate for the virus, see col. 7, lines 61-65].

wherein the information relating to the malicious code further comprises at least one command for curing a file infected with the malicious code, **recited in claims 21-24** [i.e. virus definitions of virus definition file are used for decrypting the virus and for identifying the appropriate one of overlay module, see col. 9, lines 1-16, see also, col. 8, lines 20-31 and that overlay module includes code (i.e. commands) for locating and co-opting virus repair code to restore host file (i.e. executing at least one command to restore ( and curing )) the computer system and/or infected file to the state as it existed prior to modification by the malicious code), see col. 10, lines 20-32].

**As per claims 2, 7, 12 and 17**, Nachenberg teaches wherein the step of executing the at least one command includes one of reading, writing, and deleting data [i.e., the overlay module designated in thee virus entry of the virus definition file, is written for a specific virus and includes information for locating the host bytes, and if necessary, the virus repair routine in the

virus, wherein the overlay module uses this information in conjunction with some combination of overlay, foundation, and virus repair routines to restore the host bytes to their proper locations in the host file and truncate (i.e. delete) the viral code from the host file, see col. 3, lines 27-50. The teaching of Nachenberg clearly suggests reading, writing and deleting as necessary processes to first locate (i.e. read) the host bytes and restoring the bytes to their proper location (i.e. write) and truncate (i.e. delete) the virus code].

**As per claims 5, 10, 15 and 20**, Nachenberg teaches wherein the data file comprises a plurality of data files, each data file being provided for a particular type of malicious code, each data file including at least one command that can be used for restoring the computer system to a state that existed prior to modification by the particular type of malicious code [i.e. a virus definition files (i.e. a plurality of data files) , wherein a virus Id identifies the specific virus or virus strain that ERS is being called upon to repair. Nachenberg discloses three scenarios representing some of the common strategies employed by various viruses for infecting COM, EXE, and SYS files, see col. 4, line 35 through col. 5, line 35, see also col. 7, line 65 through col. 8, line 33].

***Claim Rejections - 35 USC § 103***

3. **Claims 3, 8, 13 and 18** are rejected under 35 U.S.C. 103(a) as being unpatentable over Nachenberg as applied to claims 1, 6, 11 and 16 above, and further in view of Templeton, US Pat. 6, 401,210, filed Sep. 1998.

Nachenberg fails to teach wherein the step of executing the at least one command includes at least one of renaming and deleting a file.

However, Templeton teaches the step of executing the at least one command includes at least one of renaming and deleting a file presents a method of managing a file infected by at least one computer virus [in one embodiment, Templeton teaches a virus bin comprising a database, controlled access directory, or other data structure holding a plurality of files and information fields related to the files. Templeton teaches that an anti-virus process may be used to continually monitor a system for viruses via a memory-resident program providing real-time protection.

The anti-virus process may be used to scan one or more files in a file structure for a virus and the anti-virus process may prompt the user to select an option to deal with viruses that may be detected. the options comprise: attempt to clean the file, delete the file, rename the file, or move the file to the virus bin, see col. 3, line 40 through col. 4, line 4].

It would have been obvious to one of ordinary skill in the art to modify the repair system of Nachenberg to that of Templeton to rename and delete infected files, because deleting alone would remove the virus from the computer system, but also destroys the files original content while renaming the infected files would preserve the original content while reducing the probability of the file being accidentally used or transferred, see col. 1, lines 22-56].

4. **Claims 4, 9, 14, and 19** are rejected under 35 U.S.C. 103(a) as being unpatentable over Nachenberg as applied to claims 1, 6, 11 and 16 above, and further in view of FIXHAPPY (a Happy99.worm Removal Tool) announced by AntiVirus Research Center (IDS #5).

Nachenberg as modified fail to teach wherein the malicious code modifies at least one file and said method comprises:

reading from the modified file, a name of a second file; and

modifying the second file.

However, The Happy99.worm Removal Tool teaches reading from the modified file, a name of a second file; and

modifying the second file [ that is, restoring WSOCK32.DLL modified to hook the mail-sending and newsgroup article-posting routine. Happy99.worm Removal Tool modifies the Windows system directory by deleting SKA.EXE and SKA.DLL files and by removing windows registry modification].

It would have been obvious to one of ordinary skill in the art to modify Nachenberg's repair system to incorporate the feature taught in Happy99.warm Removal Tool to not only restore the content of infected file (s) (in system directory), but also to modify other file(s) infected (in system registry ) to reduce the spread of the worm (virus), especially when a user is online or connected to a network, see the document.

**Action is Final**

5. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however,

will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

**Conclusion**

**6.** Any inquiry concerning this communication or earlier communications from the examiner should be directed to Taghi T. Arani whose telephone number is (571) 272-3787. The examiner can normally be reached on 8:00-5:30 Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Taghi T. Arani, Ph.D.
Examiner
Art Unit 2131

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100